



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

Address: COMMISSIONER FOR PATENTS

P.O. Box 1450

Alexandria, Virginia 22313-1450

www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/863,139	05/22/2001	Roy F. Quick JR.	010055B1	1058
23696 7590 10/16/2008 QUALCOMM INCORPORATED 5775 MOREHOUSE DR. SAN DIEGO, CA 92121				
EXAMINER MOORTHY, ARAVIND K				
ART UNIT 2431		PAPER NUMBER		
NOTIFICATION DATE 10/16/2008		DELIVERY MODE ELECTRONIC		

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

us-docketing@qualcomm.com

kascanla@qualcomm.com

namn@qualcomm.com

# Office Action Summary

## Application No.

09/863,139

## Applicant(s)

QUICK ET AL.

## Examiner

Aravind K. Moorthy

## Art Unit

2431

**Period for Reply** -- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on 19 June 2008.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 1-32 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☒ Claim(s) 1-16 and 18-29 is/are allowed.
- 6) ☒ Claim(s) 17 and 30-32 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 20 August 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

## Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/C)
- 4) ☐ Interview Summary (PTO-413)
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_
- Paper No(s)/Mail Date \_\_\_\_\_

**DETAILED ACTION**

1. This is in response to the amendment filed on 19 June 2008.
2. Claims 1-32 are pending in the application.
3. Claims 1-16 and 18-29 have been allowed.
4. Claim 17 and 30-32 has been rejected.

***Response to Arguments***

5. Applicant's arguments with respect to claims 17 and 30-32 have been considered but are moot in view of the new ground(s) of rejection.

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 17 and 30-32 are rejected under 35 U.S.C. 102(b) as being anticipated by Jobst et al U.S. Patent No. 6,707,915 B1.

As to claim 17, Jobst et al discloses an apparatus for authenticating a subscriber in a wireless communication system, wherein the apparatus can be communicatively coupled to a mobile station operating within the wireless communications system, comprising:

a memory [column 5, lines 45-64]; and

a processor [column 5, lines 45-64] configured to implement a set of instructions stored in the memory [column 7, lines 3-36], the set of instructions

for selectively generates a primary signature (i.e. sig1) based upon a key (i.e. private key 64) that is held private from the mobile station [column 11, lines 32-43] and a secondary signature (i.e. sig1') that is received from the mobile station, wherein the primary signature is conveyed to the mobile station for authenticating the subscriber [column 11, lines 50-59].

As to claim 30, Jobst et al discloses a method operational on a device for authenticating a subscriber in a wireless communication system, comprising:

receiving a secondary signature (i.e. sig1') from a mobile station operating within the wireless communications system, wherein the device is configured to be communicatively coupled to the mobile station [column 11, lines 50-59]; and

generating a primary signature (i.e. sig1) based on a key (i.e. private key 64) that is held private from the mobile station and the secondary signature [column 11, lines 32-43], wherein the primary signature is conveyed to the mobile station for authenticating the subscriber [column 11, lines 50-59].

As to claim 31, Jobst et al discloses a device for authenticating a subscriber in a wireless communication system, comprising:

means for receiving a secondary signature (i.e. sig1') from a mobile station operating within the wireless communications system, wherein the device is configured to be communicatively coupled to the mobile station [column 11, lines 50-59]; and

means for generating a primary signature (i.e. sig1) based on a key (i.e. private key 64) that is held private from the mobile station and the secondary signature [column 11, lines 32-43], wherein the primary signature is

conveyed to the mobile station for authenticating the subscriber [column 11, lines 50-59].

As to claim 32, Jobst et al discloses a machine-readable medium having one or more instructions operational on a device for authenticating a subscriber in a wireless communication system, which when executed by a processor causes the processor to:

receiving a secondary signature (i.e. sig1') from a mobile station operating within the wireless communications system, wherein the device is configured to be communicatively coupled to the mobile station [column 11, lines 50-59]; and

generating a primary signature (i.e. sig1) based on a key (i.e. private key 64) that is held private from the mobile station and the secondary signature [column 11, lines 32-43], wherein the primary signature is conveyed to the mobile station for authenticating the subscriber [column 11, lines 50-59].

***Allowable Subject Matter***

7. Claims 1-16 and 18-29 are allowed.

As to independent claims 1 and 18-20, prior art does not teach or suggest the limitation "concatenating the initial value with a received signal to form an input value, wherein the received signal is transmitted from a communications unit communicatively coupled to the subscriber identification module, and the received signal is generated by the communications unit using a second key from the plurality of keys, the second key having been communicated from the subscriber identification module to the communications unit". Prior art does teach or suggest the limitation "hashing the input value to form an authentication signal". Prior art does

teach or suggest the limitation “transmitting the authentication signal to the communications system via the communications unit”.

As to independent claims 8 and 21-26, prior art does not teach or suggest the limitation “a signature generator configured to receive a secret key from the key generation element and information from a mobile unit, and further configured to generate a signature that will be sent to the mobile unit, wherein the signature is generated by concatenating the secret key with the information from the mobile unit and hashing the concatenated secret key and information [column 8, lines 32-62].

As to independent claims 11 and 27-29, prior art does not teach or suggest the limitation “a key generator for generating a plurality of keys from a received value and a secret value, wherein at least one communication key from the plurality of keys is delivered to the communications unit and at least one secret key from the plurality of keys is not delivered to the communications unit”. Prior art does teach or suggest the limitation “a signature generator for generating an authorization signal from hashing a version of the at least one secret key together with an authorization message that the authorization message is generated by the communications unit using a version of the at least one communication key”.

As to independent claim 15, prior art does not teach or suggest the limitation “generating a plurality of keys”. Prior art does teach or suggest the limitation “transmitting at least one key from the plurality of keys to a communications device communicatively coupled to the subscriber identification device and holding private at least one key from the plurality of keys”. Prior art does teach or suggest the limitation “generating a signature at the communications device using both the at least one key transmitted to the communications device and a

transmission message, wherein generating is implemented by hashing a concatenated value formed from the at least one key and the transmission message”. Prior art does teach or suggest the limitation “transmitting the signature to the subscriber identification device”. Prior art does teach or suggest the limitation “receiving the signature at the subscriber identification device”. Prior art does teach or suggest the limitation “generating a primary signature from the received signature, wherein the generating is implemented by hashing a concatenated value formed from the at least one private key and the signature received from the communications device”. Prior art does teach or suggest the limitation “conveying the primary signature to a communications system”.

Any claims not directly addressed are allowed on its virtue of dependency.

### ***Conclusion***

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Aravind K Moorthy/  
Examiner, Art Unit 2431

/Christopher A. Revak/  
Primary Examiner, Art Unit 2431